



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/820,110	03/28/2001	Ramanathan Ramanathan	42390P10983	2329

8791 7590 07/28/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER

LAFORGIA, CHRISTIAN A

ART UNIT

PAPER NUMBER

2131

DATE MAILED: 07/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/820,110

Applicant(s)RAMANATHAN, RAMANATHAN **Examiner**

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 May 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☒ Claim(s) 1-15 and 22-24 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. The amendment filed on 10 May 2004 is noted and made of record.
2. Claims 1-27 are presented for examination.

Terminal Disclaimer

3. The terminal disclaimer filed on 10 May 2004 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of U.S. Patent Application Serial #09/945,913 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Response to Arguments

4. Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.
5. See further rejections that follow.

Claim Rejections - 35 USC § 102

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
7. Claims 1, 5, 6, 10, 11, 15, 16, 18, 20, and 22-27 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,301,658 to Koehler, hereinafter Koehler.
8. As per claims 1, 6, and 11, Koehler teaches a method comprising:
writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document, see Figure 1, blocks 15, 20, 30, 35, see column 2, lines 51-67, see column 4, line 66 to column 5, line 20;

signing, by the first digital certificate issuing authority, the electronic document to obtain a once signed electronic document, see Figure 1, block 40, see column 2, lines 51-67, see column 4, line 66 to column 5, line 20;

transmitting the once signed electronic document to a second digital certificate issuing authority, see column 2, line 51 to column 3, line 3;

signing, by the second digital certificate issuing authority, the once signed electronic document to obtain a twice signed electronic document, see column 2, line 51 to column 3, line 3, see column 4, line 66 to column 5, line 20,

wherein the second digital certificate issuing authority is hierarchically superior to the first digital certificate issuing authority, column 2, lines 51-67. The bottom of column 2, gives an example of certificate chaining, wherein the marketing division issues digital certificates for any document being created by the marketing team, thereby creating a once signed electronic document. The document is then transferred to the corporate digital certificate issuing authority for further authentication, thereby creating a twice-signed document, wherein the second digital certificate issuing authority is hierarchically superior to the first digital certificate issuing authority.

9. Regarding claims 5, 10, and 15, Koehler teaches wherein writing a party's authenticating information and a first digital certificate issuing authority's authenticating information in an electronic document comprises receiving the party's authenticating information via a secure connection, see column 2, lines 28-34.

Art Unit: 2131

10. Regarding claims 22-27, Koehler discloses wherein the second digital certificate issuing authority is a root digital certificate issuing authority, refer to column 3, lines 45-60.

11. As per claims 16, 18, and 20, Koehler teaches a method comprising:

receiving, from a first digital certificate issuing authority, a once signed electronic document at a second digital certificate issuing authority that is hierarchically superior to the first digital certificate issuing authority, see column 2, line 51 to column 3, line 3;

writing the second digital certificate issuing authority's authenticating information in the once signed electronic document, see Figure 1, block 40, see column 2, lines 51-67, see column 4, line 66 to column 5, line 20; and

signing, by the second digital certificate authority, the once signed electronic document to form a twice signed electronic document, see column 2, line 51 to column 3, line 3, see column 4, line 66 to column 5, line 20.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. Claims 2-4, 7-9, 12-14, 17, 19, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Koehler in view of **Newton's Telecom Dictionary**, by Harry Newton, hereinafter Newton.

Art Unit: 2131

14. Regarding claims 2, 7, and 12, Koehler does not disclose determining a hash value and adding it to the electronic document. **Microsoft's Computer Dictionary, 5th Edition** defines a hash value as:

A value used in creating digital signatures. This value is generated by imposing a hashing algorithm onto a message. This value is then transformed, or signed, by a private key to produce a digital signature.

Newton's Telecom Dictionary further defines a hash value as:

A small amount of binary data, typically around 160 bits, derived from a message by using a hashing algorithm. The hashing procedure is one-way. There is no feasible way of deriving the original message, or even any of its properties, from the hash value, even given the hashing algorithm. The same message will always produce the same hash value when passed through the same hashing algorithm.

Thus according to the definitions provided above the determination to use a hash value includes providing, as input to a hash algorithm, the contents of the electronic document; calculating, by the hash algorithm, a hash value; encrypting the hash value using the first digital certificate issuing authority's private key; and writing the encrypted hash value in the electronic document. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a hash value in addition to the digital signature, since Newton states on page 345 that such a modification would prevent the forging of an altered message.

15. Regarding claims 3, 8, 13, 17, 19, and 21, Koehler discloses writing the second digital certificate issuing authority's authenticating information in the once signed electronic document see column 2, lines 51-67.

16. Koehler does not disclose determining a hash value and adding it to the electronic document. **Microsoft's Computer Dictionary, 5th Edition** defines a hash value as:

A value used in creating digital signatures. This value is generated by imposing a hashing algorithm onto a message. This value is then transformed, or signed, by a private key to produce a digital signature.

Art Unit: 2131

Newton's Telecom Dictionary further defines a hash value as:

A small amount of binary data, typically around 160 bits, derived from a message by using a hashing algorithm. The hashing procedure is one-way. There is no feasible way of deriving the original message, or even any of its properties, from the hash value, even given the hashing algorithm. The same message will always produce the same hash value when passed through the same hashing algorithm.

Thus according to the definitions provided above the determination to use a hash value includes providing, as input to a hash algorithm, the contents of the electronic document; calculating, by the hash algorithm, a hash value; encrypting the hash value using the second digital certificate issuing authority's private key; and writing the encrypted hash value in the electronic document. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a hash value in addition to the digital signature, since Newton states on page 345 that such a modification would prevent the forging of an altered message.

17. With regards to claims 4, 9, and 14, Koehler discloses wherein the party's authenticating information, the first digital certificate issuing authority's authenticating information, the digital signature of the first digital certificate issuing authority, and the second digital certificate issuing authority's authenticating information are all part of the document being signed multiple times, please refer to column 2, lines 51-67, and column 4, line 66 to column 5, line 20. Thus it would have required only routine skill in the art at the time the invention was made to choose one of the abovementioned identifiers to serve as input for the hash algorithm.

Claim Objections

18. Claims 1-15 and 22-24 are objected to because of the following informalities:

The independent claims cite as the last limitation "wherein the second digital issuing authority is hierarchically superior to the first digital certificate issuing authority." For the sake

Art Unit: 2131

of examination the Examiner has interpreted the claims to read as “wherein the second digital certificate issuing authority is hierarchically superior to the first digital certificate issuing authority” (Emphasis added).

19. Appropriate correction is required.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

21. The following patents are cited to further show the state of the art with respect to certificate chaining, such as:

United States Patent No. 5,903,882 to Asay et al., which is cited to show an example of certificate chains amongst certificate authorities in figure 2.

United States Patent No. 6,237,096 to Bisbee et al., which is cited to show electronic transmission of authenticated documents.

United States Patent No. 6,513,116 to Valente, which is cited to show security information acquisition.

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

23. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Art Unit: 2131

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704.


The examiner can normally be reached on Monday thru Thursday 7-5.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100